REMARKS

By this Amendment, claim 12 is canceled, without prejudice or disclaimer of the subject matter recited therein, and claims 1, 3-5, 8-10, 13-14, 17-23, 26-2 and 29-32 are amended. Therefore, claims 1, 3-10 and 13-32 are pending. Reconsideration of the application is respectfully requested.

Applicants thank Examiners Lanier and Barron for the courtesies extended to Applicants' representatives during the February 17 personal interview. During the interview, the Examiners requested clarification of the claim language to better understand the distinctions asserted by Applicants' representatives. Applicants respectfully respond to the Examiners' request by amending the claims to improve their clarity.

The Office Action rejects claims 1, 3-10, and 12-32 under 35 U.S.C. §103(a) over U.S. Patent No. 5,502,766 to Boebert et al. ("Boebert") in view of U.S. Patent No. 6,496,928 to Deo et al. ("Deo"). This rejection is moot with respect to canceled claim 12, and is respectfully traversed with respect to the remaining claims.

The Office Action states that the media shown in Fig. 19 and various elements described at col. 16, lines 4-67 of Boebert describing an embodiment relating to "Keying of Devices" correspond to the features recited in the claims. The Office Action also refers to col. 12, lines 22-24 of Boebert, which also relates to the "Keying of Devices" embodiment. Therefore, as discussed and acknowledged by the Examiners during the personal interview, Applicants respectfully understand that the Office Action intends to allege that Boebert's embodiment of "Keying of Devices" in view of Deo allegedly anticipates the features recited in the claims.

Claim 1 recites, *inter alia*, that a receiver (e.g., receiver 101) receives initial data and extracts first data and second data from the initial data, that an encryptor (e.g., encryptor 104) encrypts the first data with an encrypting key generated by the encrypting key generation unit

(e.g., key generation unit 105), and that a sender generates final data including at least one of the result of encrypting by the encryptor and the second data stored in a key generation data memory unit (e.g., key generation data memory unit 109).

By citing col. 12, lines 22-24 of Boebert, the Office Action alleges that the Media Key/Access Vector pair packet 92 that is encrypted with the Combined Key corresponds to the encryptor recited in claim 1. However, as described at col. 6, lines 39-43 of Boebert in the "Keying of Devices" embodiment, the Combined Key is formed to decrypt the Media Key/Access Vector pair packet 92, the Media Key 42 is passed to Data Crypto 74, and the Access Vector 52 is passed to Access Control Logic 76.

As explained by the Examiners at the interview, citing col. 12, lines 22-24 of Boebert is considered to disclose that the Media Key/Access Vector pair is encrypted with the Combined Key. However, as discussed during the interview, Applicants respectfully submit that this description is an error because of inconsistency with the more detailed description of the "Keying of Devices" embodiment in col. 16, lines 4-67, especially at lines 39-43 and Fig. 19 of Boebert.

The Examiners also explained that encrypted data must have been encrypted at some point and that such encryption and thus encrypted data correspond to the recited features. However, Applicants respectfully submit that the "Keying of Devices" embodiment does not teach or suggest such encryption of data.

Even if the Media Key/Access Vector pair is encrypted with the Combined Key, Boebert does not teach or suggest in the "Key of Devices" embodiment the initial data from which the Media Key and Access Vector are extracted.

Furthermore, the Office Acton states that the User ID and PIN allegedly correspond to the second data recited in the rejected claims. However, the user ID and PIN are not extracted

from the initial data from which the Media Key/Access Vector pair, which the Office Action alleges to be the first data, is extracted.

As such, Applicants respectfully assert that Boebert does not teach or suggest the features recited in claim 1. Deo does not overcome these deficiencies of Boebert. Accordingly, Applicants respectfully submit that claim 1 is patentably distinct from the applied references.

Claims 3-8 are allowable at least for their dependence on claim 1, as well as for the additional features they recite.

Claim 9 recites a feature that first data is encrypted with an encrypting key, which is similar to claim 1. For this feature, the reasoning set forth in the Office Action is similar to that presented for claim 1. That is, the Office Action alleges that the Media Key/Access Vector pair 92 is encrypted by the Combined Key 44. As discussed above, Applicants respectfully submit that neither Boebert nor Deo teaches or suggests this feature of claim 9. As such, Applicants respectfully submit that claim 9 is patentably distinct from the applied references.

Claim 10 is amended to incorporate the features of canceled claim 12 and recites that the verification unit (e.g., signature verification unit 205) checks whether the first date decrypted by the decryptor (e.g., decryptor 204) is a result of decrypting prescribed data with a prescribed decrypting key. In other words, the verification unit verifies that the decrypted first data is the prescribed data.

The Office Action alleges that the Access Control Logic 76 of Boebert corresponds to the recited verification unit. However, as described in the Office Action and col. 16, lines 57-61 of Boebert, the access control logic 76 uses the Access Vector 52 to determine whether the user has the appropriate attributes for the desired mode of access (e.g., "read" and "write"). The Access Control Logic 76 merely checks the user's attributes and does not verify whether

the decrypted Access Vector 52 is a result of decrypting prescribed data (i.e., the access vector before it was encrypted) by a prescribed decrypting key. In other words, Boebert does not teach or suggest checking the integrity of the decryption of data. During the interview, the Examiners explained that the decryption is considered to have an automatic verification function because the data would not be decrypted unless the correct information (key) is used for the decryption. Applicants respectfully disagree.

Applicants respectfully submit that although the encrypted data would not be decrypted if a wrong key is used, this does not mean that the data decrypted by a correct key provides sufficient integrity or identity of data with the data at the time it was encrypted. The feature recited in claim 10 checks if the data decrypted by the decryptor is the result of decrypting prescribed data. Boebert does not verify the accuracy of decrypted data and thus cannot achieve the advantages of the apparatus of claim 10. Deo does not overcome the deficiencies of Boebert. As such, Applicants respectfully submit that claim 10 is patentably distinct from the applied references.

Claims 13-17 are allowable at least for their dependency on claim 10, as well as for the additional features they recite.

Claim 18 is amended to incorporate features similar to claim 10. As such, claim 18 is patentably distinct from the applied references at least for the reasons set forth above with respect to claim 10.

Claim 19 recites, *inter alia*, a reference data memory unit (e.g., objective data memory unit 203) that holds first data, and a decrypting key generation unit (e.g., key generation unit 206) that generates a decrypting key from the second data stored in the first key generation data memory unit (e.g., key generation data memory unit 209). Claim 19 also recites a decryptor (e.g., decryptor 204) that decrypts the encrypted data received from the data generating apparatus with the decrypting key generated by the decrypting key generation unit,

and a verification unit (e.g., signature verification unit 205) that checks whether the data decrypted by the decryptor has a prescribed relationship with respect to integrating with the first data stored in the reference data memory unit.

The Office Action alleges that the Media Key corresponds to the first data, and that the Access Vector corresponds to the decrypted data. However, the Office Action also alleges that the Access Vector corresponds to the second data. Thus, the Office Action inconsistently relies on the Access Vector to allegedly correspond to multiple claim features.

The Office Action also alleges that the Access Control Logic corresponds to the recited verification unit. However, as stated in the Office Action, the Access Control Logic of Boebert uses the Access Vector to determine whether the user has the appropriate attributes for the desired mode of access. Boebert does not teach or suggest determining whether the Access Vector has a prescribed relationship with respect to integrity with the Media Key (alleged first data).

In addition, the Office Action alleges that the Media Key/Access Vector pair 92 described at col. 16, lines 46-67 that is ultimately used to decrypt the Media Data corresponds to the decryption key. Applicants respectfully disagree.

Claim 19 specifically recites that the data received from the data generating apparatus is decrypted with the decrypting key generated by the decrypting key generation unit. As discussed during the interview, the Media Key/Access Vector pair by itself does not decrypt the Media Data. The Media Key decrypts the Media Data (col. 16, lines 53-54). However, the Office Action alleges the Media Key/Access Vector pair corresponds to the first data. Moreover, the Media Key is not generated from the Access Vector. Accordingly, Boebert does not teach or suggest this feature.

Claim 19 also recites an encryptor (e.g., encryptor 104) that encrypts the third data with the encrypting key generated by an encrypting key generation unit (e.g., key generation unit 105).

Applicants respectfully submit that for the reasons described in relation to claim 1, Boebert does not teach or suggest this feature.

Moreover, claim 19 recites a sender (e.g., sender 102) that sends the encrypted third data to the data verifying apparatus. Applicants respectfully submit that, in Boebert, the Media Key/Access Vector, alleged to correspond to the third data, is not sent to the Media, which the Office Action alleges to correspond to the data verifying apparatus.

Deo does not overcome any of these deficiencies of Boebert. As such, for at least these reasons, Applicants respectfully submit that claim 19 is patentably distinct from the applied references.

Claims 20-29 are allowable at least for their dependency on claim 19, as well as for the additional features they recite.

Claim 30 recites that a first device (e.g., data generator 100) encrypts prescribed data received from a second device (e.g., data verifier 200) to be verified with an encrypting means on the basis of first data stored in a first data memory means (e.g., key generation data memory unit 109), and that a second device decrypts the encrypted prescribed data received from the first device to be verified with a decrypting means on the basis of second data stored in the second data memory means, verifies the integrity of a result of decrypting with the verifying means, and, if the data is successfully verified, authenticates the identity between the first data stored in the first data memory means and the second data stored in the second data memory means. That is, once the integrity of a result of decrypting with the verifying means is verified, it is confirmed that the first data and the second data are identical.

The Office Action alleges that Boebert's personal keying device 30 corresponds to the first device, and that the crypto media control 26 corresponds to the second device. The Office Action also alleges that the Media Key/Access Vector pair corresponds to the first data, and appears to assert that the Access Vector corresponds to the second data.

However, Applicants respectfully submit that Boebert does not teach or suggest that the identity of the Media Key/Access Vector pair and the Access Vector is authenticated by verifying the integrity of the result of decrypting the Media Key/Access Vector. As discussed above, Boebert merely teaches that the Access Vector is used to check whether the user has an appropriate attribute to handle the media.

In addition, col. 16, lines 30-33 describes that the enciphered Media Key/Access Vector pair packet 92 is extracted from the personal keying device 30. In other words, the personal keying device 30 contains the Media Key/Access Vector pair packet 92 that has already been enciphered. Therefore, Boebert does not teach or suggest that the personal keying device 30 generates the Media Key/Access Vector packet 92.

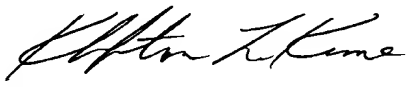
As such, Boebert does not teach or suggest the first device recited in claim 30. Deo does not overcome this deficiency of Boebert. Accordingly, claim 30 is patentably distinct from the applied references.

Claims 31 and 32 are allowable at least for their dependency on claim 30 as well as for the additional features they recite.

In view of the foregoing, it is respectfully submitted that this application is in condition for allowance. Favorable reconsideration and prompt allowance of claims 1, 3-10 and 13-32 are earnestly solicited.

Should the Examiner believe that anything further would be desirable in order to place this application in even better condition for allowance, the Examiner is invited to contact the undersigned at the telephone number set forth below.

Respectfully submitted,



James A. Oliff
Registration No. 27,075

Klifton L. Kime
Registration No. 42,733

JAO:KLK/mdw

Date: March 30, 2005

OLIFF & BERRIDGE, PLC
P.O. Box 19928
Alexandria, Virginia 22320
Telephone: (703) 836-6400

DEPOSIT ACCOUNT USE AUTHORIZATION
Please grant any extension necessary for entry;
Charge any fee due to our Deposit Account No. 15-0461